

### **Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

#### **Listing of Claims:**

1. **(Currently Amended)** An apparatus comprising a machine readable memory that provides instructions for use in encryption or decryption, for solving a system of linear equations  $Ax=b$  in  $n$  unknowns on a finite field  $GF(p)$ , where  $p$  is a prime,  $n$  is a positive integer,  $A$  is a coefficient matrix consisting of elements of  $n$  rows and  $n$  columns,  $x$  is a vector of unknowns consisting of  $n$  elements, and  $b$  is a constant vector consisting of  $n$  elements, the apparatus comprising which when executed by a machine, cause said machine to perform operations comprising:  
  
parameter storing means for storing the coefficient matrix  $A$  and the constant vector  $b$ ;  
  
triangular transforming means for reading the a stored coefficient matrix  $A$  and the a stored constant vector  $b$  from the parameter storing means, and triangular transforming the read coefficient matrix  $A$  and constant vector  $b$  to generate a coefficient matrix  $C$  and a constant vector  $d$  for a system of linear equations  $Cx=d$  in  $n$  unknowns that is equivalent to the system of linear equations  $Ax=b$ , the coefficient matrix  $C$  consisting of elements of  $n$  rows and  $n$  columns and the constant vector  $d$  consisting of  $n$  elements, wherein the coefficient matrix  $A$  is triangular transformed into the coefficient matrix  $C$  of upper triangular form without diagonal elements of the coefficient matrix  $A$  being changed to  $1$ ;  
  
diagonal element inverting means for calculating inverses of diagonal elements of the generated coefficient matrix  $C$  on the finite field  $GF(p)$ ; and  
  
equation computing means for solving the system of linear equations  $Cx=d$  using the generated coefficient matrix  $C$ , the generated constant vector  $d$ , and the calculated inverses of the diagonal elements of the generated coefficient matrix  $C$ , to thereby

solve the system of linear equations  $Ax=b$  of the read coefficient matrix  $A$  and the read constant vector  $b$ ; wherein

the coefficient matrix  $A$  is triangular transformed into the coefficient matrix  $C$  of upper triangular form without a division on the finite field  $GF(p)$  being performed.

2. (Currently Amended) The apparatus of Claim 1, wherein:

~~the triangular transforming means performs one or more successive transformation processes to generate~~ generating the coefficient matrix  $C$  and the constant vector  $d$  of the system of linear equations  $Cx=d$  from the coefficient matrix  $A$  and the constant vector  $b$  of the system of linear equations  $Ax=b$  includes one or more successive transformation processes: [[,]]

the system of linear equations  $Ax=b$  is subjected to the first transformation process and the system of linear equations  $Cx=d$  is generated as a result of the last transformation process;

~~wherein in each transformation process, the triangular transforming means transforms a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns [[,]] are transformed into a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns that is equivalent to the system of linear equations before the transformation; , where the system of linear equations  $Ax=b$  is subjected to the first transformation process and the system of linear equations  $Cx=d$  is generated as a result of the last transformation process;~~

~~wherein in each transformation process, the system of linear equations in  $n$  unknowns that is subjected to the transformation includes one pivotal equation which is a linear equation in  $n$  unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in  $n$  unknowns to be transformed are chosen from the system of linear equations in  $n$  unknowns that is subjected to the transformation;~~

each transformation process has a same number of transformation subprocesses as the one or more object equations, each for transforming a separate one of the one or more object equations into an equation equivalent to the object equation; and in each transformation subprocess,

(a) each of the coefficients and a constant in the pivotal equation is multiplied by a nonzero coefficient chosen from the object equation, and values generated as a result of the multiplications are set into a second coefficient group,

(b) each of coefficients and a constant in the object equation is multiplied by a nonzero coefficient chosen from the pivotal equation, and values generated as a result of the multiplications are set into a first coefficient group, and

(c) the values in the second coefficient group are subtracted respectively from the values in the first coefficient group, and differences generated as a result of the subtractions are respectively set as coefficients and a constant in the equation equivalent to the object equation.

~~, and the triangular transforming means transforms each of the object equations into an equation equivalent to the object equation by~~

~~defining a first coefficient group containing at least one value related to the pivotal equation and a second coefficient group containing  $n+1$  values related to the pivotal equation,~~

~~changing a nonzero coefficient in the object equation to 0, and~~

~~multiplying each of a constant and  $n$  coefficients in the object equation by the value in the first coefficient group, and subtracting the  $n+1$  values in the second coefficient group respectively from the  $n+1$  multiplication results.~~

3. (Cancelled)

4. **(Currently Amended)** The apparatus of Claim [[3]] 2, wherein

when the diagonal elements of the coefficient matrix  $C$  are denoted by  $m_i$  ( $i=1,2,\dots,n$ ) and the inverses of the diagonal elements  $m_i$  ( $i=1,2,\dots,n$ ) in the finite field  $GF(p)$  are denoted by  $I_i$  ( $i=1,2,\dots,n$ ), ~~the diagonal element inverting means~~ calculating inverses of diagonal elements of the coefficient matrix  $C$  includes

(a) ~~a multiplying unit for~~ computing values  $t$  and  $t_i$  where

$$t_i = \prod_{k=1}^n m_k \text{ (except } m_i) \bmod p \text{ (} i=1,2,\dots,n \text{)}$$

and

$$t = \prod_{k=1}^n m_k \bmod p$$

(b) ~~a first inverting unit for~~ computing  $u$  where

$$u = 1/t \bmod p$$

and

(c) ~~a second inverting unit for~~ computing values  $I_i$  where

$$I_i = u \times t_i \bmod p \text{ (} i=1,2,\dots,n \text{)}$$

to find the inverses  $I_i$  ( $i=1,2,\dots,n$ ).

5. **(Currently Amended)** The apparatus of Claim 4,

wherein ~~the multiplying unit calculates~~ computing the values  $t$  and  $t_i$  includes calculating

$$s_1 = m_1 \times m_2 \bmod p$$

$$s_2 = s_1 \times m_3 \bmod p$$

$\vdots$

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

in the stated order, then ~~calculates~~ calculating

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$t_{n-1} = s_{n-3} \times m_n \bmod p$$

$$s_n = m_{n-1} \times m_n \bmod p$$

$$t_{n-2} = s_{n-4} \times s_n \bmod p$$

$$s_{n-1} = m_{n-2} \times s_n \bmod p$$

$$t_{n-3} = s_{n-5} \times s_{n-1} \bmod p$$

$$s_{n-2} = m_{n-3} \times s_{n-1} \bmod p$$

$$t_{n-4} = s_{n-6} \times s_{n-2} \bmod p$$

⋮

$$s_5 = m_4 \times s_6 \bmod p$$

$$t_3 = s_1 \times s_5 \bmod p$$

$$s_4 = m_3 \times s_5 \bmod p$$

$$t_2 = m_1 \times s_4 \bmod p$$

$$t_1 = m_2 \times s_4 \bmod p$$

in the stated order, and lastly ~~ealeulates~~ calculating

$$t = t_j \times m_j$$

for a value  $j$  chosen from a set of positive integers  $\{1, 2, \dots, n\}$ .

6. **(Currently Amended)** The apparatus of Claim [[2]] 1 wherein:

generating the coefficient matrix  $C$  and the constant vector  $d$  of the system of linear equations  $Cx=d$  from the coefficient matrix  $A$  and the constant vector  $b$  of the system of linear equations  $Ax=b$  includes one or more successive transformation processes;

the system of linear equations  $Ax=b$  is subjected to the first transformation process and the system of linear equations  $Cx=d$  is generated as a result of the last transformation process;

in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns that is equivalent to the system of linear equations before the transformation;

in each transformation process, one pivotal equation which is a linear equation in  $n$  unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in  $n$  unknowns to be transformed are chosen from the system of linear equations in  $n$  unknowns that is subjected to the transformation;

each transformation process has a coefficient group calculation process and a same number of transformation subprocesses as the one or more object equations, the transformation subprocesses being performed following the coefficient group calculation process and being each for transforming a separate one of the one or more object equations;

in the coefficient group calculation process,

(a) a nonzero coefficient is chosen from each of the pivotal equation and the one or more object equations, a product is calculated for each of the pivotal equation and the one or more object equations by multiplying together all chosen nonzero coefficients except a nonzero coefficient chosen from the equation, and products calculated respectively for the pivotal equation and the one or more object equations are set into a first coefficient group, and

(b) each of coefficients and a constant in the pivotal equation except a nonzero coefficient chosen from the pivotal equation in the coefficient group calculation process is multiplied by a product in the first coefficient group calculated for the pivotal equation, and values generated as a result of the multiplications are set into a second coefficient group; and

in each transformation subprocess for transforming a separate one of the one or more object equations,

(a) a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to 0 as a new coefficient,

(b) each of coefficients in the object equation except the nonzero coefficient chosen from the object equation is multiplied by a product in the first coefficient group calculated for the object equations, values in the second coefficient group calculated from the coefficients in the pivotal equation are subtracted respectively from values generated as a result of the multiplications on the coefficients in the object equation to generate differences, and the coefficients in the object equation are changed respectively to the differences as new coefficients, and

(c) a constant in the object equation is multiplied by the product calculated for the object equations, a value in the second coefficient group calculated from the constant in the pivotal equation is subtracted from a value generated as a result of the multiplication on the constant in the object equation to generate a difference, and the constant in the object equation is changed to the difference as a new constant.

~~, wherein each transformation process has a coefficient group calculation process and transformation subprocesses, performed following the coefficient group calculation process, each for transforming a separate one of the object equations,~~

~~wherein in the coefficient group calculation process the triangular transforming means~~

~~(a) — chooses  $m$  nonzero coefficients by taking one nonzero coefficient from each of the pivotal equation and the object equations, multiplies each combination of  $(m-1)$  of the chosen nonzero coefficients, and sets the  $m$  multiplication results into the first coefficient group,  $m$  being a positive integer no smaller than 2, and~~

~~(b) — multiplies each of a constant and  $n$  coefficients in the pivotal equation by a multiplication result in the first coefficient group for a combination of~~

~~nonzero coefficients that does not include a nonzero coefficient chosen from the pivotal equation, and sets  $n+1$  values obtained by the multiplications into the second coefficient group, and~~

~~wherein in each of the transformation subprocesses following the coefficient group calculation process, the triangular transforming means~~

- ~~(a) — changes a nonzero coefficient chosen from the object equation in the coefficient group calculation process, to 0 in the object equation, and~~
- ~~(b) — multiplies each of a constant and  $n$  coefficients in the object equation by a multiplication result in the first coefficient group for a combination of nonzero coefficients that does not include the nonzero coefficient chosen from the object equation, and subtracts the  $n+1$  values in the second coefficient group respectively from the  $n+1$  multiplication results.~~

7. **(Currently Amended)** The apparatus of Claim [[6]] 2,

wherein when the diagonal elements of the coefficient matrix  $C$  are denoted by  $m_i$  ( $i=1,2,...,n$ ) and the inverses of the diagonal elements  $m_i$  ( $i=1,2,...,n$ ) in the finite field  $GF(p)$  are denoted by  $I_i$  ( $i=1,2,...,n$ ) , the diagonal element inverting means calculating inverses of diagonal elements of the coefficient matrix  $C$  includes

- (a) a multiplying unit for computing values  $t$  and  $t_i$  where

$$t_i = \prod_{k=1}^n m_k \text{ (except } m_i) \text{ mod } p \text{ (} i=1,2,\dots,n \text{)}$$

and

$$t = \prod_{k=1}^n m_k \text{ mod } p$$

- (b) ~~a first inverting unit for computing a value  $u$  where~~

$$u=1/t \text{ mod } p$$

and



(c) a second inverting unit for computing values  $I_i$  where

$$I_i = u \times t_i \bmod p \quad (i=1,2,\dots,n)$$

to find the inverses  $I_i$  ( $i=1,2,\dots,n$ ).

8. (Currently Amended) The apparatus of Claim 7,

wherein ~~the multiplying unit calculates~~ computing values  $t$  and  $t_i$  includes calculating

$$s_1 = m_1 \times m_2 \bmod p$$

$$s_2 = s_1 \times m_3 \bmod p$$

⋮

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

in the stated order, then ~~calculates~~ calculating

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$t_{n-1} = s_{n-3} \times m_n \bmod p$$

$$s_n = m_{n-1} \times m_n \bmod p$$

$$t_{n-2} = s_{n-4} \times s_n \bmod p$$

$$s_{n-1} = m_{n-2} \times s_n \bmod p$$

$$t_{n-3} = s_{n-5} \times s_{n-1} \bmod p$$

$$s_{n-2} = m_{n-3} \times s_{n-1} \bmod p$$

$$t_{n-4} = s_{n-6} \times s_{n-2} \bmod p$$

⋮

$$s_5 = m_4 \times s_6 \bmod p$$

$$t_3 = s_1 \times s_5 \bmod p$$

$$s_4 = m_3 \times s_5 \bmod p$$

$$t_2 = m_1 \times s_4 \bmod p$$

$$t_1 = m_2 \times s_4 \bmod p$$

in the stated order, and lastly ~~calculates~~ calculating

$$t = t_j \times m_j$$

for a value  $j$  chosen from a set of positive integers  $\{1, 2, \dots, n\}$ .

9. **(Currently Amended)** An apparatus ~~for use in encryption or decryption~~, for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q = p^n$ , and  $n$  is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax = b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax = b$ , the equation solving means including

the apparatus of Claim 1; and

inverse computing means for computing the inverse  $I, I = x_0 + x_1\alpha + \dots + x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

10. **(Currently Amended)** An apparatus ~~for use in encryption or decryption~~, for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q = p^n$ , and  $n$  is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax = b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax = b$ , the equation solving means including the apparatus of Claim 2; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

11. **(Currently Amended)** ~~An apparatus for use in encryption or decryption,~~ for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q=p^n$ , and  $n$  is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 3; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

12. **(Currently Amended)** ~~An apparatus for use in encryption or decryption,~~ for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q=p^n$ , and  $n$  is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 4; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

13. **(Currently Amended)** An apparatus ~~for use in encryption or decryption~~, for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q=p^n$ , and  $n$  is a positive integer, the apparatus comprising:
- equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;
- equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 5;
- and
- inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.
14. **(Currently Amended)** An apparatus ~~for use in encryption or decryption~~, for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q=p^n$ , and  $n$  is a positive integer, the apparatus comprising:
- equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;
- equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 6;
- and
- inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.
15. **(Currently Amended)** An apparatus ~~for use in encryption or decryption~~, for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q=p^n$  and  $n$  is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 7; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

16. **(Currently Amended)** An apparatus ~~for use in encryption or decryption~~, for computing an inverse  $I$  of an element  $y$  in  $GF(q)$  which is an extension field of a finite field  $GF(p)$ , where  $p$  is a prime,  $q=p^n$ , and  $n$  is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 8; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

17. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,

$q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 1; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

18. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,  $q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 2; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

19. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,  $q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 3; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

20. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,  $q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 4; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

21. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,  $q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 5; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

22. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,



$q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 6; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

23. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,  $q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 7; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

24. **(Currently Amended)** A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve  $E$  over  $GF(q)$  as a basis for security and recorded on a record medium, an inverse  $I$  of an element  $y$  in  $GF(q)$  to decrypt the encrypted digital content recorded on the record medium, where  $GF(q)$  is an extension field of a finite field  $GF(p)$ ,  $p$  is a prime,  $q=p^n$ ,  $n$  is a positive integer, and  $G$  is a base point of the elliptic curve  $E$ , the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix  $A$  and a constant vector  $b$  for a system of linear equations  $Ax=b$  in  $n$  unknowns, using the element  $y$  and all coefficients of a generator polynomial of  $GF(q)$  whose root is  $\alpha$ ;

equation solving means for finding solutions  $x_k (k=0, 1, 2, \dots, n-1)$  of the system of linear equations  $Ax=b$ , the equation solving means including the apparatus of Claim 8; and

inverse computing means for computing the inverse  $I, I=x_0+x_1\alpha+\dots+x_{n-1}\alpha^{n-1}$ , using the root  $\alpha$  and the solutions  $x_k (k=0, 1, 2, \dots, n-1)$  found by the equation solving means.

25. **(Currently Amended)** A machine based method for solving a system of linear equations  $Ax=b$  in  $n$  unknowns on a finite field  $GF(p)$  where  $p$  is a prime,  $n$  is a positive integer,  $A$  is a coefficient matrix consisting of elements of  $n$  rows and  $n$  columns,  $x$  is a vector of unknowns consisting of  $n$  elements, and  $b$  is a constant vector consisting of  $n$  elements, ~~for use in encryption or decryption in an apparatus equipped with parameter storing means which stores the coefficient matrix  $A$  and the constant vector  $b$~~ , the method comprising:

utilizing a machine readable memory to provide instructions to a machine for execution by the machine, wherein

the instructions, when executed by the machine, cause the machine to perform operations comprising:

~~a triangular transforming step for reading the a stored coefficient matrix  $A$  and the a stored constant vector  $b$  from the parameter storing means, and triangular transforming the read coefficient matrix  $A$  and constant vector  $b$  to generate a coefficient matrix  $C$  and a constant vector  $d$  for a system of linear equations  $Cx=d$  in  $n$  unknowns that is equivalent to the system of linear equations  $Ax=b$ , the coefficient matrix  $C$  consisting of elements of  $n$  rows and  $n$  columns and the constant vector  $d$  consisting of  $n$  elements, wherein the coefficient matrix  $A$  is triangular transformed into the coefficient matrix  $C$  of upper triangular form without diagonal elements of the coefficient matrix  $A$  being changed to 1;~~

~~a diagonal element inverting step for calculating inverses of diagonal elements of the generated coefficient matrix  $C$  on the finite field  $GF(p)$ ; and~~

~~an equation computing step for solving the system of linear equations  $Cx=d$  using the generated coefficient matrix  $C$ , the generated constant vector  $d$ , and the calculated inverses of the diagonal elements of the generated coefficient matrix  $C$ , to thereby solve the system of linear equations  $Ax=bi$  of the read coefficient matrix  $A$  and the read constant vector  $b$ , wherein~~

the coefficient matrix  $A$  is triangular transformed into the coefficient matrix  $C$  of upper triangular form without a division on the finite field  $GF(p)$  being performed.

26. (Currently Amended) The method of Claim 25, wherein:

~~the triangular transforming step includes one or more successive transformation processes to generate generating the coefficient matrix  $C$  and the constant vector  $d$  of the system of linear equations  $Cx=d$  from the coefficient matrix  $A$  and the constant vector  $b$  of the system of linear equations  $Ax=b$  includes one or more successive transformation processes;~~

the system of linear equations  $Ax=b$  is subjected to the first transformation process and the system of linear equations  $Cx=d$  is generated as a result of the last transformation process,

~~wherein~~ in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns that is equivalent to the system of linear equations before the transformation, ~~where the system of linear equations  $Ax=b$  is subjected to the first transformation process and the system of linear equations  $Cx=d$  is generated as a result of the last transformation process,~~

~~wherein~~ in each transformation process, ~~the system of linear equations in  $n$  unknowns that is subjected to the transformation includes one pivotal equation which is a linear equation in  $n$  unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in  $n$  unknowns to be transformed are chosen from the system of linear equations in  $n$  unknowns that is subjected to the transformation;~~

each transformation process has a same number of transformation subprocesses as the one or more object equations, each for transforming a separate one of the one or more object equations into an equation equivalent to the object equation; and in each transformation subprocess,

- (a) each of the coefficients and a constant in the pivotal equation is multiplied by a nonzero coefficient chosen from the object equation, and values generated as a result of the multiplications are set into a second coefficient group,
- (b) each of coefficients and a constant in the object equation is multiplied by a nonzero coefficient chosen from the pivotal equation, and values generated as a result of the multiplications are set into a first coefficient group, and
- (c) the values in the second coefficient group are subtracted respectively from the values in the first coefficient group, and differences generated as a result of the subtractions are respectively set as coefficients and a constant in the equation equivalent to the object equation.

~~, and each of the object equations is transformed into an equation equivalent to the object equation by~~

~~defining a first coefficient group containing at least one value related to the pivotal equation and a second coefficient group containing  $n+1$  values related to the pivotal equation;~~

~~changing a nonzero coefficient in the object equation to 0, and~~

~~multiplying each of a constant and  $n$  coefficients in the object equation by the value in the first coefficient group, and subtracting the  $n+1$  values in the second coefficient group respectively from the  $n+1$  multiplication results.~~

27. (Cancelled)

28. (Currently Amended) The method of Claim [27] 26, wherein

when the diagonal elements of the coefficient matrix  $C$  are denoted by  $m_i$  ( $i=1,2,\dots,n$ ) and the inverses of the diagonal elements  $m_i$  ( $i=1,2,\dots,n$ ) in the finite field  $GF(p)$  are denoted by  $I_i$  ( $i=1,2,\dots,n$ ), calculating the inverses of the diagonal elements of the coefficient matrix  $C$  ~~the diagonal element inverting means~~ includes

(a) ~~a multiplying unit for computing~~ values  $t$  and  $t_i$  where

$$t_i = \prod_{k=1}^n m_k \text{ (except } m_i) \bmod p \text{ (} i=1,2,\dots,n)$$

and

$$t = \prod_{k=1}^n m_k \bmod p$$

(b) ~~a first inverting unit for computing~~ value  $u$  where

$$u = 1/t \bmod p$$

and

(c) ~~a second inverting unit for computing~~ values  $I_i$  where

$$I_i = u \times t_i \bmod p \quad (i=1, 2, \dots, n)$$

to find the inverses  $I_i \quad (i=1, 2, \dots, n)$ .

29. **(Currently Amended)** The method of Claim 28,

wherein the ~~multiplying substep calculates~~ computing the values  $t$  and  $t_i$  includes  
calculating

$$s_1 = m_1 \times m_2 \bmod p$$

$$s_2 = s_1 \times m_3 \bmod p$$

⋮

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

in the stated order, then ~~calculates~~ calculating

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$t_{n-1} = s_{n-3} \times m_n \bmod p$$

$$s_n = m_{n-1} \times m_n \bmod p$$

$$t_{n-2} = s_{n-4} \times s_n \bmod p$$

$$s_{n-1} = m_{n-2} \times s_n \bmod p$$

$$t_{n-3} = s_{n-5} \times s_{n-1} \bmod p$$

$$s_{n-2} = m_{n-3} \times s_{n-1} \bmod p$$

$$t_{n-4} = s_{n-6} \times s_{n-2} \bmod p$$

⋮

$$s_5 = m_4 \times s_6 \bmod p$$

$$t_3 = s_1 \times s_5 \bmod p$$

$$s_4 = m_3 \times s_5 \bmod p$$

$$t_2 = m_1 \times s_4 \bmod p$$

$$t_1 = m_2 \times s_4 \bmod p$$

in the stated order, and lastly ~~ealeulates~~ calculating

$$t = t_j \times m_j$$

for a value  $j$  chosen from a set of positive integers  $\{1, 2, \dots, n\}$ .

30. **(Currently Amended)** The method of Claim [26,] 25, wherein:

generating the coefficient matrix  $C$  and the constant vector  $d$  of the system of linear equations  $Cx=d$  from the coefficient matrix  $A$  and the constant vector  $b$  of the system of linear equations  $Ax=b$  includes one or more successive transformation processes;

the system of linear equations  $Ax=b$  is subjected to the first transformation process and the system of linear equations  $Cx=d$  is generated as a result of the last transformation process;

in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in  $n$  unknowns that is equivalent to the system of linear equations before the transformation;

in each transformation process, one pivotal equation which is a linear equation in  $n$  unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in  $n$  unknowns to be transformed are chosen from the system of linear equations in  $n$  unknowns that is subjected to the transformation;

each transformation process has a coefficient group calculation process and a same number of transformation subprocesses as the one or more object equations, the transformation subprocesses being performed following the coefficient group calculation process and being each for transforming a separate one of the one or more object equations;

in the coefficient group calculation process,

- (a) a nonzero coefficient is chosen from each of the pivotal equation and the one or more object equations, a product is calculated for each of the pivotal equation and the one or more object equations by multiplying together all chosen nonzero coefficients except a nonzero coefficient chosen from the equation, and products calculated respectively for the pivotal equation and the one or more object equations are set into a first coefficient group, and
- (b) each of coefficients and a constant in the pivotal equation except a nonzero coefficient chosen from the pivotal equation in the coefficient group calculation process is multiplied by a product in the first coefficient group calculated for the pivotal equations, and values generated as a result of the multiplications are set into a second coefficient group; and
- in each transformation subprocess for transforming a separate one of the one or more object equations,
- (a) a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to 0 as a new coefficient,
- (b) each of coefficients in the object equation except the nonzero coefficient chosen from the object equation is multiplied by a product in the first coefficient group calculated for the object equations, values in the second coefficient group calculated from the coefficients in the pivotal equations are subtracted respectively from values generated as a result of the multiplications on the coefficients in the object equation to generate differences, and the coefficients in the object equation are changed respectively to the differences as new coefficients, and
- (c) a constant in the object equation is multiplied by the product calculated for the object equations, a value in the second coefficient group calculated from the constant in the pivotal equation is subtracted from a value generated as a result of the multiplication on the constant in the object equation to generate a difference, and the constant in the object equation is changed to the difference as a new constant.



~~wherein each transformation process includes a coefficient group calculation process and transformation subprocesses, performed following the coefficient group calculation process, each for transforming a separate one of the object equations, wherein in the coefficient group calculation process~~

- ~~(a) —  $m$  nonzero coefficients are chosen by taking one nonzero coefficient from each of the pivotal equation and the object equations, each combination of  $(m-1)$  of the chosen nonzero coefficients is multiplied, and the  $m$  multiplication results are set into the first coefficient group,  $m$  being a positive integer no smaller than 2, and~~
- ~~(b) — each of a constant and  $n$  coefficients in the pivotal equation is multiplied by a multiplication result in the first coefficient group for a combination of nonzero coefficients that does not include a nonzero coefficient chosen from the pivotal equation, and  $n+1$  values obtained by the multiplications are set into the second coefficient group,~~

~~wherein in each of the transformation subprocesses following the coefficient group calculation process~~

- ~~(a) — a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to 0 in the object equation, and~~
- ~~(b) — each of a constant and  $n$  coefficients in the object equation is multiplied by a multiplication result in the first coefficient group for a combination of nonzero coefficients that does not include the nonzero coefficient chosen from the object equation, and the  $n+1$  values in the second coefficient group are subtracted respectively from the  $n+1$  multiplication results.~~

31. (Currently Amended) The method of Claim [30]26, wherein

when the diagonal elements of the coefficient matrix  $C$  are denoted by  $m_i$  ( $i=1,2,\dots,n$ ) and the inverses of the diagonal elements  $m_i$  ( $i=1,2,\dots,n$ ) in the finite field  $GF(p)$  are denoted by  $I_i$  ( $i=1,2,\dots,n$ ), calculating the inverses of the diagonal elements of the coefficient matrix  $C$  ~~the diagonal element inverting means~~ includes

- (a) ~~a multiplying unit for~~ computing values  $t$  and  $t_i$  where

$$t_i = \prod_{k=1}^n m_k \text{ (except } m_i) \bmod p \text{ (} i=1, 2, \dots, n)$$

and

$$t = \prod_{k=1}^n m_k \bmod p$$

- (b) ~~a first inverting unit for~~ computing a value  $u$  where

$$u = 1/t \bmod p$$

and

- (c) ~~a second inverting unit for~~ computing values  $I_i$  where

$$I_i = u \times t_i \bmod p \text{ (} i=1, 2, \dots, n)$$

to find the inverses  $I_i$  ( $i=1, 2, \dots, n$ ).

32. **(Currently Amended)** The method of Claim 31,

wherein ~~the multiplying substep calculates~~ computing values  $t$  and  $t_i$  involves calculating

$$s_1 = m_1 \times m_2 \bmod p$$

$$s_2 = s_1 \times m_3 \bmod p$$

$\vdots$

$$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$$

in the stated order, then ~~calculates~~ calculating

$$t_n = s_{n-3} \times m_{n-1} \bmod p$$

$$t_{n-1} = s_{n-3} \times m_n \bmod p$$

$$s_n = m_{n-1} \times m_n \bmod p$$

$$t_{n-2} = s_{n-4} \times s_n \bmod p$$

$$s_{n-1} = m_{n-2} \times s_n \bmod p$$

$$t_{n-3}=s_{n-5}\times s_{n-1} \bmod p$$

$$s_{n-2}=m_{n-3}\times s_{n-1} \bmod p$$

$$t_{n-4}=s_{n-6}\times s_{n-2} \bmod p$$

$\vdots$

$$s_5=m_4\times s_6 \bmod p$$

$$t_3=s_1\times s_5 \bmod p$$

$$s_4=m_3\times s_5 \bmod p$$

$$t_2=m_1\times s_4 \bmod p$$

$$t_1=m_2\times s_4 \bmod p$$

in the stated order, and lastly calculates calculating

$$t=t_j\times m_j$$

for a value  $j$  chosen from a set of positive integers  $\{1,2,\dots,n\}$ .